

DATA, INFORMATION AND VIDEO FOOTAGE

| | |
|---|---|
| <p>New Era of Public Safety (3/28/2019)</p> | <p>Part I:</p> <p>Collect and publish demographic and enforcement data. This includes data about stops, searches, summonses, arrests, and uses of force. Each officer should be assigned a unique identifier so departments can link officer-involved incidents to other data, such as misconduct complaints, while concealing officers' identities (for privacy and due process concerns). Departments should also analyze and maintain demographic and enforcement data to identify possible patterns of biased policing, misallocation of resources, or inadequate training. p. 239, pdf p. 277. Departments should also provide data about the volume and nature of complaints. p. 240, pdf p. 278</p> <p>Police should not use data collection technologies to collect and store large amounts of data about members of the public. p. 236, pdf p. 274. Departments should not collect private information (such as personal characteristics, associations, or activities) or use technologies that risk infringing on civil and human rights. p. 237, pdf p. 275.</p> <p>Make data and information publicly available in accessible and alternative formats. Online versions of long policy manuals should contain searchable tables of contents. p. 241, pdf p. 279. Communities and police departments should explore how to present aggregate data in a way that promotes true transparency through information dashboards, maps, graphical interfaces that use icons, menus, and other visual graphics, and the like. They should also make raw data available for download so researchers, academics, and other interested parties can access and analyze it. p. 242-243, pdf p. 280-281.</p> <p>Procure adequate systems to collect and store data. Databases should be linked because 'Siloed' databases make it difficult to identify patterns of behavior by officers and departments. Departments should also track information about officer performance through computer-aided dispatch (CAD) systems, record management systems (RMS), or other performance databases. p. 244, pdf p. 282.</p> <p>Release information about critical events in a timely manner. Department leaders should work with community members, elected officials, local prosecutors, officer organizations, crime victims' representatives, and others to develop policies around the release of information about critical incidents. When possible, leaders should also release existing BWC and dashboard camera (a.k.a. "dashcam") footage. p. 244-245, pdf p. 282-283.</p> <p>Develop clear BWC policies with community input. Clearly state when officers are required to activate BWCs. Departments should require officers to record all encounters with safeguards to protect privacy and preserve community relationships. BWC policies should also define what is meant by 'encounters,' provide examples of them, and clearly state exceptions, such as recording lawful behavior (e.g., political or religious activity and conversations with confidential informants or child victims). Department leaders should detail consequences for noncompliance and require officers to provide written justifications when they violate BWC policies. p. 247-248, pdf p. 285-286.</p> |
| <p>New Era of Public Safety Cont'd (3/28/2019)</p> | <p>Part II:</p> <p>Train officers to use and maintain BWCs. Officers should, for example, be trained to immediately activate BWCs at the beginning of encounters unless otherwise directed (e.g., when in contact with a child victim). BWCs should record 30 seconds of video (though typically not audio) prior to activation . . . Training should also cover the responsibilities for and restrictions on using BWCs, such as informing people that they are being recorded (again, when possible). Training should also include practices to ensure (1) the integrity of recordings; (2) that the footage 'chain of custody' is documented (i.e., who has possessed the footage and whom they have passed it along to and when); and (3) disciplinary action for improperly editing, erasing, copying, sharing, altering, or distributing camera footage. p. 248, pdf p. 286.</p> <p>Develop policies around the release of video footage. In general, departments should release video footage to those seeking to file a complaint and to next of kin in police-caused fatalities. Privacy concerns should be addressed before footage is released to broad, public audiences. p. 248, pdf p. 287.</p> <p>Departments should implement policies for supervisory review and periodic audits of BWC footage. p. 250, pdf p. 288.</p> <p>Prohibit the use of facial recognition software with BWC footage. p. 251, pdf p. 289.</p> <p>Implement storage practices and systems to preserve the integrity of video footage. In general, departments should delete footage that hasn't been flagged (e.g., footage that's related to an investigation) after six months. Policies should also include provisions to preserve data related to criminal investigations until cases are closed. Once footage is stored, departments should have a cybersecurity plan in place to protect it. p. 252, pdf p. 290.</p> |
| <p>21st Century Policing (5/2015)</p> | <p>Part I:</p> <p>"Law enforcement agencies should collaborate with community members, especially in communities and neighborhoods disproportionately affected by crime, to develop policies and strategies for deploying resources that aim to reduce crime by improving relationships, increasing community engagement, and fostering cooperation. To achieve this end, law enforcement agencies should have clear and comprehensive policies on the use of force (including training on the importance of de-escalation), mass demonstrations (including the appropriate use of equipment, particularly rifles and armored personnel carriers), consent before searches, gender identification, racial profiling, and performance measures—among others such as external and independent investigations and prosecutions of officer-involved shootings and other use of force situations and in-custody deaths. These policies should also include provisions for the collection of demographic data on all parties involved. All policies and aggregate data should be made publicly available to ensure transparency." p. 2, pdf pp 16.</p> <p>"Expanded research and data collection are also necessary to knowing what works and what does not work, which policing practices are effective and which ones have unintended consequences." p. 19-20, pdf pp 33-34.</p> <p>"Policies on use of force should . . . require agencies to collect, maintain, and report data to the Federal Government on all officer-involved shootings, whether fatal or nonfatal, as well as any in-custody death." p. 21, pdf pp 35.</p> <p>"[L]aw enforcement agencies should adopt model policies and best practices for technology-based community engagement that increases community trust and access." p. 3, pdf pp 17.</p> <p>"Law enforcement agencies should encourage public engagement and collaboration, including the use of community advisory bodies, when developing a policy for the use of a new technology." p. 35, pdf pp 49. "[C]oncerns about [technology such as body cameras] include potential compromises to the privacy of both officers and citizens, who are reluctant to speak to police if they think they are being recorded. . . . '[H]aving the conversation can increase trust and legitimacy and help departments make better decisions.'" Id.</p> <p>"[A]dopt model policies and best practices for technology-based community engagement that increases community trust and access." p. 36, pdf pp 50. "These policies and practices should at a minimum increase transparency and accessibility, provide access to information (crime statistics, current calls for service), allow for public posting of policy and procedures, and enable access and usage for persons with disabilities." Id. "[T]o engage the community, social media must be responsive and current." Id.</p> <p>"[D]evelop policies and practices on social media use that consider individual officer expression, professional representation, truthful communication, and other concerns that can impact trust and legitimacy." p. 36, pdf pp 50.</p> |
| <p>21st Century Policing Cont'd. (5/2015)</p> | <p>Part II:</p> <p>"Law enforcement agencies should establish a culture of transparency and accountability in order to build public trust and legitimacy. This will help ensure decision making is understood and in accord with stated policy." p. 12, pdf pp 26. More specifically, "law enforcement agencies should make all department policies available for public review and regularly post on the department's website information about stops, summonses, arrests, reported crime, and other law enforcement data aggregated by demographics." p. 13, pdf pp 27.</p> <p>"[C]ollect, maintain, and analyze demographic data on all detentions (stops, frisks, searches, summons, and arrests). This data should be disaggregated by school and non-school contacts." p. 13, pdf pp 27. More specifically, "[m]ore research and tools along the lines of Lorie Fridell's 2004 publication, By the Numbers: A Guide for Analyzing Race Data From Vehicle Stops—to help local agencies collect and analyze their data, understand the importance of context to the analysis and reporting process, and establish benchmarks resulting from their findings—would improve understanding and lead to evidence-based policies." Id.</p> <p>"All federal, state, local, and tribal law enforcement agencies should report and make available to the public census data regarding the composition of their departments including race, gender, age, and other relevant demographic data." p. 24, pdf pp 38.</p> <p>"Law enforcement agencies should encourage public engagement and collaboration, including the use of community advisory bodies, when developing a policy for the use of a new technology," such as BWCs. p. 35, pdf pp 49. "[C]oncerns about BWCs include potential compromises to the privacy of both officers and citizens, who are reluctant to speak to police if they think they are being recorded. . . . '[H]aving the conversation can increase trust and legitimacy and help departments make better decisions.'" Id.</p> <p>"[R]eview and consider the Bureau of Justice Assistance's (BJA) Body Worn Camera Toolkit to assist in implementing BWCs." p. 36, pdf pp 50.</p> |
| <p>Report on Police Reform and Racial Justice (8/2020)</p> | <p>Police departments should use body-worn cameras if not already doing so. p. 29, pdf p. 31.</p> <p>Policies and trainings should provide clear, easy-to-understand directions for how to use body-worn cameras and when they must be activated. p. 29, pdf p. 31.</p> <p>Departments should create clear protocols for the use of body-worn camera footage in officer investigations, and for the review and release of that footage to the public, consistent with applicable public records retention and disclosure laws. The time period for disclosure should be set in advance, by policy. Ideally, disclosure is automatic in the case of officer-involved shootings (provided no privacy concerns are implicated). Policies should clearly prohibit any alteration of footage by department personnel. p. 29, pdf p. 31.</p> <p>Departments should implement an audit function to monitor the use of body-worn cameras and ensure adherence to department policies. p. 29, pdf p. 31.</p> |

| | |
|---|---|
| <p>Redefining Policing With Our Community (5-8/2020)</p> | <p>Make information on use-of-force incidents, including all relevant geographic and demographic data, publicly available and accessible, and report this data at public forums such as oversight meetings and town halls. p 6, pdf p 7. See also p 31, pdf p 32.</p> <p>Integrate evaluation metrics for trainings to ensure intended behavior changes. p 8, pdf p 9.</p> <p>Provide ongoing psychological evaluation throughout an officer's career arc to ensure that work-related traumas are understood and addressed. p 8, pdf p 9. See also pp 41-42, pdf pp 42-43.</p> <p>Integrate the socio-emotional wellbeing of officers into performance evaluation metrics. p 8, pdf p 9. See also pp 41-42, pdf pp 42-43.</p> <p>Eliminate predictive surveillance practices and publically release footage from body-worn cameras and other surveillance technologies. See p 9, pdf p 10. See also p 47, pdf p 48.</p> |
| <p>Automated License Plate Reader Report (2/2020)</p> | <p>Part I: The Audit Report found that all four of the law enforcement agencies reviewed (LAPD, Fresno, Marin, and Sacramento) are in noncompliance with SB 34 in certain aspects.</p> <p><u>Noncompliant ALPR Policies:</u> -All four agencies have failed to include information about the individuals who have access to the ALPR system, and how the agency will monitor the use of the ALPR system to ensure the security of the ALPR data. -LAPD is the only agency that has not developed an ALPR policy. The LAPD claims that the requirements for an ALPR policy are covered by other IT policies that cover the ALPR program. However, according to the Auditor Report, the LAPD began drafting an ALPR-specific policy in October 2019. -The other agencies also indicated that they would consider making the necessary changes to their ALPR policies to be in compliance with the legal requirements.</p> <p><u>Inadequate Protection for ALPR Data:</u> The Audit Report recommends using the CJIS policy to govern the protection of ALPR data. CJIS policy requires that any contracts with vendors who have access to ALPR systems include provisions to adequately protect criminal justice information. -Fresno, Marin, and Sacramento store their ALPR data in a vendor's cloud database (Vigilant). The Auditor Report found that these agencies did not have sufficient data security safeguards in their contracts with Vigilant. Specifically, the agencies' respective contracts with Vigilant failed to specify how the data is stored and who can access the data, despite Vigilant's assurances of data protection. -LAPD stores its ALPR data in a city-controlled data center rather than in a vendor cloud. Nevertheless, the LAPD was not able to demonstrate that it has an agreement with its IT support vendor, Palantir, to protect its ALPR data from inappropriate access. LAPD should have an agreement with Palantir that includes specific security safeguards.</p> <p><u>Failure to Implement Proper Data Sharing Mechanisms:</u> The Audit Report could not determine whether the four agencies made informed decisions about the sharing of ALPR images. -Fresno, Marin, and Sacramento share their ALPR images through Vigilant. Each of these agencies share images with at least 500 agencies across the United States. These agencies also rely on Vigilant for sharing their ALPR images. However, these agencies have had difficulty understanding when and how sharing occurred because the information on the Vigilant user interface has changed over time. The Auditor Report noted that this type of unrestricted and uncontrolled sharing does not guarantee that the ALPR images will be used appropriately and therefore, may threaten individuals' privacy. -LAPD limits its sharing of ALPR images with entities within a regional system (related to funding from a federal grant). The LAPD shares ALPR images with 58 agencies in the Southern California region who use the same software (so that it could maintain greater control over its ALPR images). The Auditor Report noted that each authorized share exposes the ALPR image to a greater risk of misuse so agencies should evaluate each sharing request based on the requester's actual need for the images rather than issuing blanket approvals.</p> |
| <p>Automated License Plate Reader Report Cont'd (2/2020)</p> | <p>Part II: <u>Failure to Implement Proper ALPR Data Retention Policies:</u> The Audit Report found that the four agencies do not base their decisions regarding retention of ALPR images and data on the actual use by investigators, and may be retaining the images longer than necessary. While SB 34 does not mandate a specific retention period, it does require agencies to specify in their ALPR policy the length of the time ALPR data will be retained and the process the agency will use to determine if and when to destroy ALPR data. -Fresno Police Department's policy is to retain ALPR images for a minimum of one year; -LAPD's policy is to retain ALPR images for a minimum of five years pursuant to the city's Administrative Code; -Marin County Sheriff's Office's policy is to retain ALPR images for two years; and -Sacramento County Sheriff's Office's policy is to retain images for a minimum of two years. -None of the agencies considered the image's utility over time when establishing these data retention schedules: Fresno, Marin, and Sacramento searched for ALPR images zero to six months old a majority of the time; LAPD searches for images over a year old about half the time, however a majority of the searches were for images captured within the last two years. LAPD still has an overly broad data retention policy. -The Audit Report recommends that these four agencies consider both the usefulness of the ALPR images and individuals' privacy when deciding how long to retain the images. For example, agencies should consider the general dates of searches to determine the appropriate retention schedule most useful to the investigators.</p> <p><u>Inadequate Internal Safeguards to Protect Against Misuse:</u> Each of the four agencies failed to follow one or more best practices related to user access to the ALPR system. -None of the agencies had a requirement that supervisors approve staff requests for creating ALPR user accounts. -LAPD was particularly lax in implementing the proper safeguards (four total). For example, LAPD includes the ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system may have access to the system. The only safeguard it implemented was the deletion of an account once the employee left the police department.</p> <p>Best Practices: 1. Supervisor approval is a prerequisite for account access 2. ALPR training is a prerequisite for account access. 3. Accounts defined as "inactive" are suspended. 4. ALPR training is required for users linked to inactive accounts to regain active status. 5. Accounts are deleted when employees separate from the agency.</p> <p>The Audit Report recommends that each of the four agencies implement all five best practices. The Audit Report also recommends that agencies conduct audits to review the searches its users conduct in the ALPR systems.</p> |
| <p>Statement of Policing Project Regarding Policing in the United States (2020)</p> | <p>N/A</p> |
| <p>Racial Identity Profiling Advisory Board 2019 Report (2019)</p> | <p>N/A</p> |
| <p>Police Use of Force: An Examination of Modern Policing Practices (11/15/2018)</p> | <p>Part I: "Congress should condition cities' receipt of federal law enforcement funds on the cities' collection and reporting to DOJ of data regarding police use of force practices, in a format that is aggregable and comparable nationally, which DOJ can then report to the American public. Congress should require DOJ to create and maintain a public, national database of police use of force incidents and appropriate funds sufficient to support the creation and maintenance of the database." P. 139, PDF p. 149. "Congress should also require DOJ to release to the public twice each year the names of departments and jurisdictions that fail to report use of force information in the manner DOJ requires. The public release should be directed to the state Attorney General, City Council, County Commission, or other governing body overseeing the departments in the State and jurisdiction where the department administrative office resides, and DOJ should maintain the information on its website." P. 139, PDF p. 149. "Departments should provide aggregate information to the public regarding the numbers of allegations and type of use of force and what steps, if any, departments take to address use of force concerns when they arise. This data should be disaggregated by race, gender and disability status." P. 142, PDF p. 152.</p> <p>Put "plans in place to handle the large amounts of recorded data and storage of potentially sensitive information," to avoid perception "that body-worn cameras are going to result in a tradeoff between accountability and privacy." P. 69, PDF p. 79.</p> <p>"[E]stablishing civilian review boards that are truly independent and separate from law enforcement and have subpoena power is also essential." P. 73, PDF p. 83. "[H]ighly effective civilian review boards have the following elements: • The authority to investigate or review complaints of human rights violations by the public against the police; • The ability to conduct regular audits of police internal complaints and disciplinary process and, where necessary, conduct their own investigations; • The power to require witnesses to appear and to insist on cooperation from police departments and individual officers; • The authority to require police agencies to provide information on action taken in individual cases, with reasons for inaction; • The authority to review and make recommendations on policy and training; and • Provide detailed public reports, at least annually, giving relevant data, including the type of complaint and the race and gender of the complainant and the accused officer." P. 75, PDF p. 85.</p> <p>The "appointment of a Compliance Director [can] ensure that the suggested police reforms [are] carried out accordingly." Id.</p> <p>"Federal consent decrees should remain in place, but if they do not, cities and state attorneys general should take "an active role to implement reform policies without the aid of the federal government or the binding agreement of a consent decree." P. 94, PDF p. 104. Some of the accountability measures to instate include: • Prohibiting racial and other forms of discriminatory profiling; • Mandating greater transparency and accountability in police-community relations; • Establishing new protections for juveniles, immigrants, and transgender people; and • Establishing how police officers will document and collect data from traffic and pedestrian stops." Pp. 94-95, PDF pp. 104-105.</p> |

| | |
|--|---|
| <p>Police Use of Force: An Examination of Modern Policing Practices Cont'd (11/15/2018)</p> | <p>Part II:</p> <p>"Department policies should make clear that citizens have a constitutional right to film the police from a distance that does not interfere with the officer performing her/his duty. Officers should be trained on safe interactions with members of the public who desire to film them." P. 140, PDF p. 150.</p> <p>"Police departments should deploy body-worn cameras and voice recorders to capture interactions between police and citizens and should develop policies for their use. The DOJ should continue to collect model policies and make them available in an easily accessible database. Body-worn camera policies should address the following:</p> <ul style="list-style-type: none"> • Clearly defined penalties should attach for the misuse of camera footage and violations of body-worn camera policies. • Officers should not be given any knowledge of the contents and should not be given the right to view footage before making a report of the incident. • The public should be allowed to obtain footage of use of force incidents after investigations are complete. • Body-worn camera policies should also address privacy concerns raised by the large amounts of data recorded by those cameras containing potentially sensitive information deserving of individual policies. These policies should include but not be limited to footage not depicting use of force, detention, an incident subject to complaint, or that has no evidentiary, exculpatory, or training value." Pp. 141-42, PDF pp. 151-52. <p>"[P]olice officers must be prohibited from viewing the footage before filing their reports in order to preserve the independent value of their evidence . . . police footage should be logged in a server, and access to the footage should be limited to ensure the independent evidentiary value of an officer's recollection of the events . . . Officers should not see police-operated camera footage before filing their reports, because such pre-report viewing effectively eliminates the officer's independent recollection of the event as a source of evidence." P. 70, PDF p. 80.</p> <p>"[T]he truth—and the officer's credibility—are better served if an officer is not permitted to review footage of an incident prior to making a statement." P. 71, PDF p. 81.</p> <p>Require body-worn cameras. Pp. 63-72, PDF pp. 73-82. Require them to be turned on at the beginning of an encounter, because turning them on once an incident is underway can destroy their "civilizing effect" and actually escalate the situation. P. 65, PDF p. 75. Ensure enforcement of these requirements. Pp. 66-68, PDF pp. 76-78.</p> |
| <p>Strategies for Change: Research Initiatives and Recommendations to Improve Police-Community Relations in Oakland, Calif. (6/20/2016)</p> | <p>"Body-worn camera footage should be analyzed like data, so that patterns can be shown across incidents in the aggregate, instead of only analyzing it as evidence after a problem." P. 14, PDF p. 15.</p> <p>"Continue collecting stop data." P. 43, PDF p. 44. "Add a field on the stop data form to capture squad information [to] allow analysts to measure how much stop outcomes vary by the squad's experience level, gender diversity, racial diversity, and so forth." Id. "Add a field on the stop data form to capture squad sergeant information [to] allow researchers to examine how squad sergeants influence officers [and] to examine the relative contributions of officer experience and squad sergeant to the decisions officers are making about who to stop, search, handcuff, or arrest." Id. "Update the stop data form as needed." P. 44, PDF p. 45. "Standardize, track, and analyze crime-related communications provided to officers" to control the influence on officers' stop outcomes. Id.</p> <p>"Add a field on the stop data form regarding BWC usage" where officers can indicate whether their camera was on and if not, why not. P. 45, PDF p. 46. "Tag BWC footage [to allow] the department and researchers to associate each stop in the database with the BWC footage from that stop." Id. "Use BWC footage to train officers," including in best practices. Id. Require officers to self-audit racially charged BWC footage. Id. "Use BWC footage to evaluate policies." P. 46, PDF p. 47. "Invest in the development of a BWC early warning system," including PRIME, which uses "a suite of metrics to determine which officers may be having trouble and which may be likely to have trouble in the near future." Id.</p> <p>"Build a stop data dashboard . . . that clearly summarizes and visualizes stop data"; this allows command staff to "quickly glean trends, explore their own hypotheses, and develop sophisticated predictive algorithms." P. 47, PDF p. 48. "Automate stop data analyses [to] efficiently produce reports." Id. "Automate narrative analyses" and work with researchers to develop algorithms "to explore why officers stop, search, handcuff, and take other actions." Id. "Assist researchers in building an automatic speech recognition system for BWC footage [to] allow the department to examine officers' language precisely and systematically, and then develop strategies for improving officer communication." Id. "Improve systems for backing up and accessing BWC footage." P. 48, PDF p. 49.</p> <p>"Hire a data manager . . . to oversee databases, data requests, research collaborations, and data for risk management." P. 48, PDF p. 49. "Partner with outside researchers to analyze and use data." Id. "Partner with outside researchers to conduct high-quality studies." Id.</p> <p>Have risk management meetings once monthly with command staff from each area of department to compare stop data for the area to department-wide stop data over a six-month period, break down stop metrics by race and discuss trends, compare squads to one another, etc. P. 54, PDF p. 55. "Identify outlier officers . . . who are at risk of developing problematic behaviors or have already done so." Id. "Monitor and reduce time pressure," including by introducing daily activity tracking sheets. P. 55, PDF p. 56.</p> <p>"Monitor and reduce stress and fatigue," including with trainings focusing on health and wellness; examine how these factors "influence officer decision-making during police-initiated stops could uncover patterns and suggest improvements, as has happened in medicine, law, and other high-stress fields." Id. "Identify factors associated with high- and low-performing squads . . . to examine how much these performance differences are due to the individual officer characteristics, squad characteristics, squad supervisors, and the directives officers receive from command staff." Id. Review policy: Handcuffing people undergoing a search. Id. Review policy: Searching people who are on probation or parole. P. 56, PDF p. 57. Review practice: Asking people whether they are on probation or parole; using severe legal language. Id. "Produce and publish an annual Racial Impact Report" on stop data. Id. "Analyze data for trends over time." P. 57, PDF p. 58.</p> |
| <p>An Assessment of Traffic Stops and Policing Strategies in Nashville (date unknown)</p> | <p>"[R]educe the number of stops, as well as tracking, remaining conscious of, and working to eliminate as much as possible any disparity. That is true for reasons of racial justice, but also for reasons of overall public safety." P. 12, PDF p. 12. "[R]elatively few officers perform a very high number of stops, which may facilitate bringing down the number of stops." Id.</p> |